



OASD C3I



AFCEA Roundtable DoD PKI Interoperability

Moderator:

Mr. Richard Schaeffer, OASD(C3I), Director I&IA

DoD and Guest Panel:

CAPT Ted Case, Co-Director DoD Paperless Contracting

LCDR Paul Friedrichs, DISA, Chief Engineer for PKI

Mr. R. Michael Green, Director DoD PKI PMO

Mr. Richard Guida, Chair Federal PKI SC

Mr. Robert Weilminster, Navy, CNO PKI Action Officer



OASD C3I

Agenda

- Panel Briefings (45 min)
 - Developments in PKI Policy
 - DoD PKI Program Status
 - Target Class 4 Strategy
 - IECA / Vendor Interoperability
 - Class 3 Interoperability Issues
 - Federal Bridge Certification Authority
 - Electronic Business Implementation Issues
 - Service Implementation Issues
- Open Session on Above Topics



OASD C3I



Draft Policy Changes

- CAC becomes the primary hardware token for Class 3 and Target Class 4 certificates
 - Accelerates use of COTS hardware tokens
 - Does not preclude use of other approved token technologies
- Software tokens phased out.
- DEERS/RAPIDS becomes the primary mechanism for PKI registration
 - Allows PKI LRAs to fill gaps in DEERS/RAPIDS coverage
- Clarifies intent to migrate to certificate-based access control mechanisms on DoD networks
- Clarifies applicability of non-SCI classified systems

Draft Policy Changes (cont'd)

Milestone	Current Policy	Proposed Policy
<p>Server certificates (Class 3 minimum) for all DoD private web servers.</p> <p><u>Rationale for change:</u> Performance issues in some installations; Allows time to upgrade. The definition of private web server was unclear.</p>	Jun 00	Dec 00
<p>Registration Infrastructure FOC</p> <p><u>Rationale for slip:</u> DEERS/RAPIDS FOC will not occur until Dec 01. Accommodates CAC registration fielding.</p>	Oct 00	Dec 01
<p>All DoD users issued Class 3 certificates; all internal DoD e-mail digitally signed; all DoD and DoD-interest private web servers require client ID and authentication (Class 3).</p> <p><u>Rationale for slip:</u> Provides time to complete Class 3 registration using DEERS/RAPIDS as primary registration workstation.</p>	Oct 01	Oct 02

Draft Policy Changes (cont'd)

Milestone	Current Policy	Proposed Policy
Target Class 4 IOC <u>Rationale for slip:</u> Avoids overlap with baseline Class 3 certificate issuance.	Jan 02	Oct 02
All mission critical users issued Target Class 4 certs <u>Rationale for slip:</u> Ensures consistency with evolving GIG definitions of mission critical users; accommodates slippage in Class 4 issuance date as proposed above.	Dec 02	Dec 03
Cease issuing Class 3 certificates <u>Rationale for slip:</u> Some DoD military and civilians may not need Class 4, and interoperability issues remain to be worked with trading partners. Change allows more gradual Class 3 phaseout.	Jan 02	Dec 04



OASD C3I

Summary

- Draft PKI policy update in DoD-wide coordination
- Synchronizes PKI and Common Access Card activities and milestones
- Accelerates DoD-wide adoption of COTS hardware tokens
- Goal is still single, interoperable, high assurance PKI, but...
 - Allows more graceful transition from Class 3 to Target Class 4 as requested by CINCs/Services/Agencies